Partial Listing

US006105134A

United States Patent [19]

Pinder et al.

[11] **Patent Number: 6,105,134**

[45] **Date of Patent: *Aug. 15, 2000**

[54] **VERIFICATION OF THE SOURCE OF PROGRAM INFORMATION IN A CONDITIONAL ACCESS SYSTEM**

[75] Inventors: **Howard G. Pinder**, Norcross; **Michael S. Palgon**, Atlanta; **Glendon L. Akins, III**, Gainesville; **Robert O. Banker**, Cumming, all of Ga.

[73] Assignee: **Scientific-Atlanta, Inc.**, Norcross, Ga.

[*] Notice: This patent issued on a continued prosecution application filed under 37 CFR 1.53(d), and is subject to the twenty year patent term provisions of 35 U.S.C. 154(a)(2).

[21] Appl. No.: **09/126,795**

[22] Filed: **Jul. 31, 1998**

Related U.S. Application Data

[63] Continuation of application No. 08/767,535, Dec. 16, 1996, Pat. No. 6,005,938, and a continuation-in-part of application No. 08/415,617, Apr. 3, 1995, Pat. No. 5,742,677.

[60] Provisional application No. 60/054,575, Aug. 1, 1997, abandoned.

[51] **Int. Cl.**^{7} **H04L 9/32**; H04N 7/167

[52] **U.S. Cl.** **713/170**; 713/168; 380/241; 380/239; 380/279

[58] **Field of Search** 380/20, 239, 241, 380/279, 281, 283, 284; 713/168, 170, 171

[56] **References Cited**

U.S. PATENT DOCUMENTS

Re. 33,189	3/1990	Lee et al.	380/20
Re. 34,954	5/1995	Haber et al. .	
4,405,829	9/1983	Rivest et al. .	
4,531,020	7/1985	Wechselberger et al. .	

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

752786	1/1997	European Pat. Off. .

OTHER PUBLICATIONS

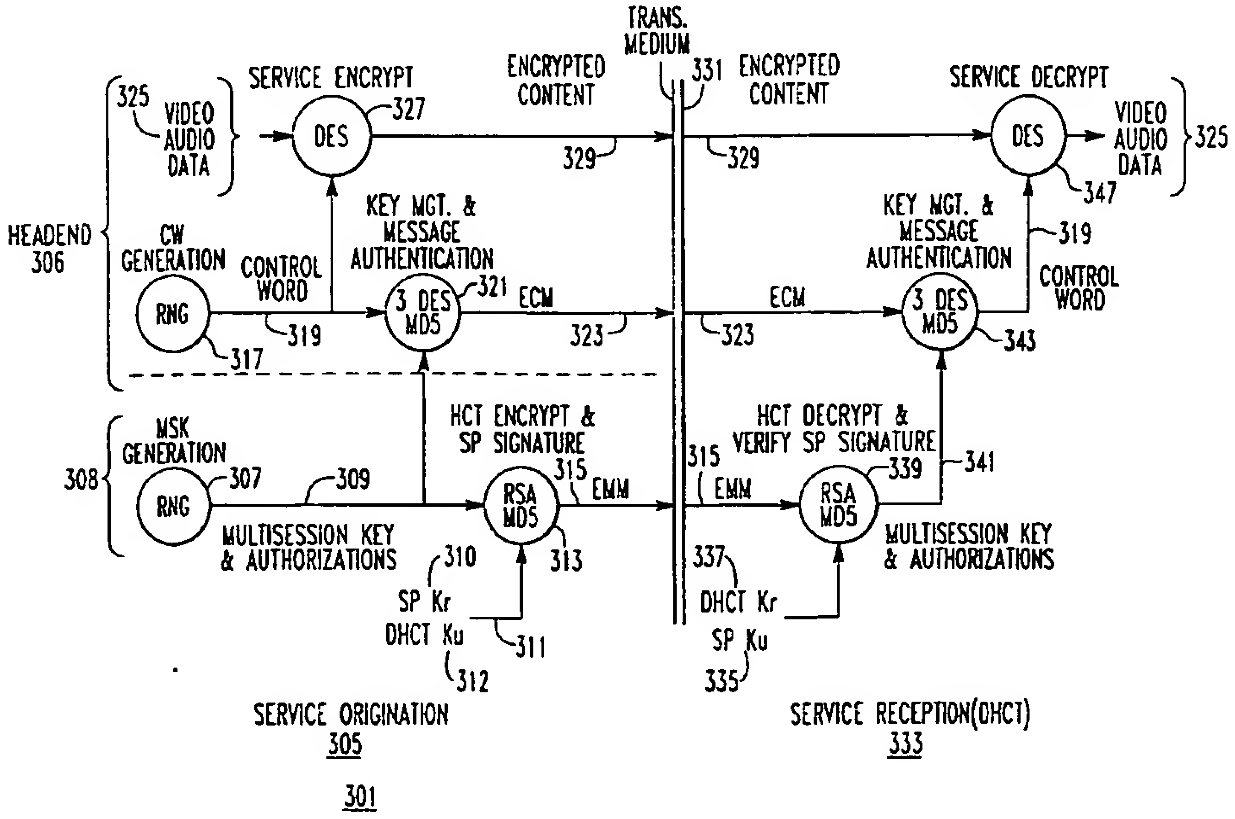
ISO IEC 31818–1, Information Technology—Generic Coding of Moving Pictures and Associated Audio: Systems, Draft Nov. 13, 1994.

Primary Examiner—Gilberto Barron, Jr.
Attorney, Agent, or Firm—Hubert J. Barnhardt, II; Kenneth M. Massaroni; Kelly A. Gardner

[57] **ABSTRACT**

A cable television system provides conditional access to services. The cable television system includes a headend from which service "instances", or programs, are broadcast and a plurality of set top units for receiving the instances and selectively decrypting the instances for display to system subscribers. The service instances are encrypted using public and/or private keys provided by service providers or central authorization agents. Keys used by the set tops for selective decryption may also be public or private in nature, and such keys may be reassigned at different times to provide a cable television system in which piracy concerns are minimized.

17 Claims, 21 Drawing Sheets



US-PAT-NO: **6105134**

DOCUMENT-IDENTIFIER: US 6105134 A

TITLE: Verification of the source of program information in a conditional access system

---------- KWIC ---------

6105134

FIG. 5 is a block diagram of a **digital broadband delivery** system in which the conditional access system is implemented;

FIG. 6 is a block diagram of the conditional access system in the **digital broadband delivery** system of FIG. 5;

Implementation of the Conditional Access System in a **Digital Broadband Delivery** System

The foregoing has described the conditional access system in terms of ECMs, EMMs, and other messages and in terms of the manner in which the messages and
their digests are encrypted and decrypted. The conditional access system as just described will work with any communications arrangement which permits an instance of a service to be delivered to a DHCT together with ECMs and other broadcast messages and which permits the DHCT to receive EMMs from a conditional access authority and one or more entitlement agents. The conditional access system is, however, particularly well-suited for use in a modem **digital broadband delivery** system, and the following will describe how the conditional access system is implemented in such a delivery system.

Overview of the **Digital Broadband Delivery** System: FIG. 5

FIG. 5 provides an overview of **digital broadband delivery** system (DBDS) 501.
DBDS 501 includes service infrastructure 503, a headend 515, a transport infrastructure 517, hubs 519 (0 . . . n), access networks 521 (0 . . . n), and Digital Home Communications Terminals (DHCTs) 333. The service infrastructure consists of Value-Added Service Provider (VASP) systems 509,

which are systems that provide services to the broad band delivery system, the Digital Network Control System (DNCS) 507, which manages and controls services provided by means of DBDS 501, the Administrative Gateway (AG) 505, which is a source of service provisioning and authorization information in DBDS 501, Network Management System (NMS) 511, which maintains a database of system status and performance information, and the Core Network 513, which interconnects other Service Infrastructure 503 components with headend 515. In a preferred embodiment, Core Network 513 consists of ATM-based switching and transmission facilities. Headend 515 provides an interface between service infrastructure 503 and transport infrastructure 517. Transport infrastructure 517 provides a high-bandwidth interconnection from headend 515 to hubs 519(0 . . . n). Each hub 519(i) serves an access network 521(i), which consists of hybrid fiber coax (HFC) nodes 523 connected via a coax bus network to DHCTs 333. A given DHCT 333(k) in DBDS 501 thus belongs to an HFC node 532(j) in an access network 521(i). Transport infrastructure 517 and access network 523 may provide only a forward channel from head end 515 to a given DHCT 333(k), but preferably provide both a forward channel and a reverse path. Each instance of a DBDS 501 generally provides service to a metropolitan area.

In **digital broadband delivery** system 501, CA messages may travel either in a MPEG-2 data stream or in an IP packet, that is, a packet made according to the rules of the Internet Protocol. Also, other transport protocols such as ATM may be used. In the preferred embodiment, messages from control suite 607 to DHCT 333 may travel in MPEG-2 or IP packets; messages from DHCT 333 to control suite 607 travel as IP packets on the reverse path provided by QPSK demodulator 623 and LAN interconnect device 617. In general, messages to DHCT 333 which are closely associated with particular instances of services, such as ECMs and GBAMs, travel in the MPEG-2 data stream; EMMs may travel either in the MPEG-2 transport stream or as IP packets via LAN interconnect device 617 and QPSK modulator 621.

DHCTSE 627 ignores EMMs that are addressed to a CAA or EA that is not "known" by DHCTSE 627 (i.e., EMMs for which there is no CAA corresponding to the CAAID or EA that corresponds to the EAID). As will be explained in more detail below, information about individual entitlements is contained in NVSCs 1211 for the entitlements. Each of these NVSCs has a type, and an EA may change the type or contents of an NVSC 1211 by sending an EMM which specifies the name of the NVSC 1211 to be altered. DHCTSE 627 will alter the NVSC 1211 as indicated in the EMM unless the entitlement agent does not have an NVSC with that name or the change violates a constraint set by the CAA. In those cases, the EMM is ignored by DHCTSE 627. Conditional access system 601 does not require that **digital broadband delivery** system 501 have a reverse path, or, if one exists, that any bandwidth on the reverse path be available to the EMM conditional access function. Consequently, DHCT 333 does not return any acknowledgment, confirmation, or error messages in response to an EMM. Therefore, the CAA or EA that is the source of an EMM should track the allocations of NVSCs 1211 and send only EMMs that request legal operations. In other embodiments, a reverse path may be required, and for these embodiments, the reverse path can be used for acknowledgment or error messages.

GBAM 1801 can be used generally to broadcast authenticated messages via a MPEG-2 transport stream, or other transport mechanisms, to DHCTs 333. CA system 601 itself uses GBAM 1801 in two other ways: to periodically broadcast a time value to DHCTs 333 and to extend the time for events. In the former case. GBAM 1801 simply carries the time value, which is a secure time, due to the GBAM's authentication. The code in DHCT 333 which carries out a task for the entitlement agent that sent the system time GBAM can use the time value to coordinate its activities with activities by the EA. Note that this arrangement permits the use of per-entitlement agent time schemes. It also permits establishing a uniform system time throughout a **digital broadband delivery** system by setting up one entitlement agent in each DHCT 333 of the **digital broadband delivery** system as the "system time entitlement agent" and addressing the system time GBAM to the system time entitlement agent.

Each CAA that can authorize entitlement agents in **digital broadband delivery** system 501 and each EA that can grant entitlements in system 501 has a Transaction Encryption Device or TED 603 in system 501. Preferably, each CAA or EA has its own separate TED in system 601. Alternatively, the TEDs could be combined in one device. The TED 603 stores the secret keys used by the entity to which it belongs and has hardware and software to do encryption, decryption, key generation, and authentication as required by the entity. The keys are kept secure by implementing the TED without a user interface or user I/O devices, by implementing it in a tamper resistant container, by connecting the TED only to the DNCS and using a secure link for that connection, and by keeping the TED in a physically secure environment such as a locked room.

FIG. 24 shows the relationship between a number of TEDs 603 and the rest of conditional access system 601. Portion 2401 of conditional access system 601 includes a CAA TED 2427 for a CAA that authorizes entitlement agents in system 601. Portion 2401 also includes one EA TED 2425 for each of the n+1 entitlement agents which the CAA has currently authorized for DHCTs 333 in **digital broadband delivery** system 501. Alternatively, all EA TED 2425 functions could be combined into a single TED, which could include the CAA TED 2427 function. Each TED is kept in a physically secure area 2428 and is connected to DNCS 507 by a secure high-speed link 2423 that connects only DNCS 507 and the TEDs 603. In the preferred embodiment, the secure link is a secure Ethernet link. DNCS 507 uses TED 605 to encrypt EMMs, to decrypt FPMs, to generate EA public and private keys, to generate MSKs and ISKs, and to prepare global broadcast message digests. DNCS 607 has a remote procedure call interface to the TEDs 603 for performing these operations, and, consequently, programs executing on DNCS 607 can use the facilities of a TED simply by making a procedure call.